

1 entering into a secure connection with a server computer;  
2 obtaining a session key specific to the secure connection;  
3 receiving data encrypted with the session key from the server computer;  
4 storing the encrypted data on a persistent storage; and  
5 securing the session key with a storage key.  
6  
7

### 8 REMARKS

9 In view of the following remarks, Applicant respectfully requests  
10 reconsideration and allowance of the subject application. No new matter is added  
11 by any amendment. Amendments made to claims 1, 2, 8, 11, 12 and 18-22 are not  
12 made for the purpose of patentability with respect to any prior art of record, and  
13 such amendments do not affect the allowability of allowed claims 18-22.  
14

### 15 Drawings

16 The Draftsperson has objected to Figures 1, 4, 5, 7A and 10 of the drawings  
17 under 37 CFR §1.84, indicating the top margins are not acceptable. The  
18 Draftsperson has also objected to Figures 2-11 of the drawings under 37 CFR  
19 §1.84, indicating that lines, numbers and letters are not uniformly thick and well  
20 defined. The Draftsperson has also objected to Figures 1B-11 of the drawings  
21 under 37 CFR §1.84, indicating that the Figure legends are poor. As indicated  
22 above, Figures 1A, 1B, 2, 3, 4, 5, 6, 7A, 7B, 7C, 8, 9, 10 and 11 are submitted  
23 herewith in a set of formal drawings. The set of formal drawings addresses the  
24 Draftsperson's objections so that Figures 1A, 1B, 2, 3, 4, 5, 6, 7A, 7B, 7C, 8, 9, 10  
25 and 11 comply with 37 CFR §1.84.

1  
2 **§102 Rejections**

3           **Claims 1-2, 5, 13-14 and 23-24** are rejected under 35 U.S.C.  
4 §102(b) as allegedly being anticipated by Herbert (US # 5,757,919). Applicant  
5 respectfully traverses the rejection.

6           Herbert discloses a “method and system for maintaining integrity and  
7 confidentiality of pages paged to an external storage unit from a physically secure  
8 environment” (col. 1, lines 58-60). The context of Herbert’s disclosure is a single  
9 computer system in which virtual memory uses external memory devices (e.g.,  
10 hard disk drives or magnetic tape) to “ameliorate the physical memory constraints  
11 of the RAM and create the appearance that adequate space is available in the RAM  
12 to hold all the currently needed code and data” (col. 1, lines 17-23). Generally,  
13 virtual memory permits a computer to execute a program that is too large to fit  
14 into the main memory (i.e., RAM) all at once. The computer executes such a  
15 program by “paging” or “swapping” blocks (e.g., 4 kilobyte pages) of code or data  
16 between RAM and external memory as needed during program execution. (col. 1,  
17 lines 19-35). Thus, Herbert discloses a way of maintaining the integrity and  
18 confidentiality of pages paged between RAM in a physically secure environment  
19 and a memory device in an external insecure environment. (col. 1, lines 58-62).

20           Herbert discusses ways of creating a physically secure environment such as  
21 tamper-resistant packaging materials, tamper-resistant die coatings and tamper-  
22 resistant wafer coatings used to create secure semiconductor devices and other  
23 secure electronic circuitry. Herbert further describes a physically secure  
24 environment that includes a processor coupled by a bus to a RAM. Within the  
25 physically secure environment is an integrity check engine that generates a hash

1 value when data is paged out of the secure environment. The hash value is “stored  
2 within the secure environment as an integrity check value (ICV) for later  
3 comparison when that page of data is subsequently paged back in” (col. 2, lines  
4 25-63).

5 In rejecting **claim 1**, the Office asserts among other things, that Herbert  
6 teaches a computerized method for key-based secure storage comprising  
7 downloading content and an access predicate that specifies requirements for an  
8 application to access the content. However, as made clear from the following  
9 discussion, this is not the case.

10 In contrast to Herbert’s system for secure paging between a secure  
11 environment and an external memory, Applicant’s **claim 1** recites “downloading  
12 information and an access predicate that specifies requirements for an application  
13 to access the content”. Herbert does not discuss downloading information.  
14 Herbert’s disclosure relates to paging pages of code or data to facilitate a virtual  
15 memory system within a computer. Herbert discloses a “method and system for  
16 maintaining integrity and confidentiality of pages paged to an external storage unit  
17 from a physically secure environment” (col. 1, lines 58-60). Herbert states that the  
18 “functioning of paging systems is generally well understood in the art” (col. 1,  
19 lines 38-40). It is therefore clear that the term “paging” as described in Herbert  
20 (col. 1, lines 13-50) and as well understood in the art of virtual memory systems  
21 does not mean “downloading” as recited in Applicant’s claim 1.

22 Furthermore, Herbert does not discuss an “access predicate” as recited in  
23 Applicant’s claim 1. The access predicate “specifies requirements for an  
24 application to access the [downloaded] information”. By contrast, Herbert  
25 discusses an “integrity check value (ICV)”. Herbert’s ICV does not specify

1 requirements for an application to access downloaded information. Rather, the  
2 ICV is used to check the integrity of a page of data previously paged out of the  
3 physically secure environment that is being paged back into the physically secure  
4 environment. This provides “security from substitution and modification attacks  
5 of programs and data beyond the memory capacity of a secure environment”  
6 (Herbert, col. 1, lines 51-55). Herbert’s ICV, used to check the integrity of data  
7 being paged back into a physically secure environment, is nothing at all like an  
8 “access predicate that specifies requirements for an application to access the  
9 [downloaded] information” as recited in Applicant’s claim 1.

10 Moreover, even if Herbert’s ICV could be likened to Applicant’s access  
11 predicate, Herbert does not discuss downloading an access predicate. As  
12 discussed above, Herbert does not download anything. Rather, Herbert pages code  
13 or data within a computer, which is a function well known in the art of virtual  
14 memory systems. However, it is additionally noteworthy that Herbert does not  
15 even page the ICV out of the physically secure environment. The ICV does not  
16 leave the physically secure environment of Herbert. The ICV is “stored within the  
17 secure environment . . . for later comparison when [a] page of data is subsequently  
18 paged back in” (col. 2, lines 60-63). Thus, Herbert’s ICV is not even paged out of  
19 the physically secure environment, let alone downloaded to another computer.  
20 Storing an ICV in the physically secure environment as described in Herbert is in  
21 no way the same as “downloading . . . an access predicate that specifies  
22 requirements for an application to access the information” as recited in  
23 Applicant’s claim 1.

24 It is therefore clear that Herbert does not teach “downloading information  
25 and an access predicate that specifies requirements for an application to access the

1 information” as recited in Applicant’s claim 1. For at least the reasons discussed  
2 above, claim 1 is not anticipated by Herbert, and the §102(b) rejection of claim 1  
3 should be withdrawn.

4 **Claims 2, 5 and 13** depend from claim 1. Because claim 1 is allowable as  
5 discussed above, claims 2, 5 and 13 are also allowable by virtue of at least their  
6 dependency from claim 1. Applicant therefore respectfully requests withdrawal of  
7 the §102(b) rejection to dependent claims 2, 5 and 13.

8 Furthermore, with respect to claim 2, the Office states that Herbert teaches  
9 (at col. 7, lines 5-22) decrypting the content for access by an application only if  
10 the application meets the requirements specified in the access predicate. The  
11 Office again implies that Herbert’s ICV is the same as Applicant’s access  
12 predicate, which as clarified above, is not the case. Assuming for the sake of  
13 discussion, however, that Herbert’s ICV is the same as Applicant’s access  
14 predicate, Herbert still does not teach “decrypting the information for access by an  
15 application only if the application meets the requirements specified in the access  
16 predicate” as the Office asserts. In Herbert, the incoming page is already  
17 decrypted before the ICV’s are compared. In fact, the incoming page is decrypted  
18 and then hashed to determine the ICV (col. 7, lines 12-18). Thus, the ICV does  
19 not provide requirements that determine whether the page will or will not be  
20 decrypted. Likewise, the “key” and “IV” of Herbert do not provide requirements  
21 that determine whether the page will or will not be decrypted. For these additional  
22 reasons, claim 2 is not anticipated by Herbert, and the §102(b) rejection of claim 2  
23 should be withdrawn.

24 In rejecting **claim 14**, the Office asserts that Herbert teaches (at col. 3, lines  
25 2-8 and col. 2, lines 39-45) a generate key function executed from a computer-

1 readable medium by a processing unit, wherein the generate key function causes  
2 the processing unit to generate an operating system storage key based on an  
3 identity for the operating system. However, Herbert's Figure 1 and corresponding  
4 discussion at col. 2, line 39 through col. 3, line 5 make clear that this is not an  
5 accurate interpretation of Herbert's teaching.

6 Herbert specifies a "random number generator 18 . . . to generate keying  
7 material for the encryption engine 12". Although Herbert teaches a physically  
8 secure environment 1 that contains a processor 16, Herbert does not teach "a  
9 generate key function executed from [a] computer-readable medium by the  
10 processing unit". The random number generator 18 of Herbert is not a generate  
11 key function executed from a computer-readable medium. Figure 1 makes clear  
12 that Herbert's random number generator 18 is distinct from both the processor 16  
13 and any computer-readable medium (i.e., RAM 14, flash memory 15).

14 Furthermore, the keying material in Herbert is generated for the encryption  
15 engine 12 (col. 3, lines 1-3). Encryption keys are used to decrypt pages being  
16 paged back into the physically secure environment from external storage (col. 7,  
17 lines 9-12). Thus, the encryption keys in Herbert are related to whatever  
18 encryption algorithm is used to encrypt outgoing pages. By contrast, Applicant's  
19 claim 14 recites "an operating system storage key based on an identity for the  
20 operating system". Herbert does not discuss an operating system storage key that  
21 is generated based on an identity for the operating system. Herbert's encryption  
22 keys are based on an encryption algorithm, not on the identity of an operating  
23 system.  
24  
25

1 For at least the reasons discussed above, it is clear that Herbert does not  
2 teach the elements of Applicant's claim 14. Applicant therefore respectfully  
3 requests that the §102(b) rejection of claim 14 be withdrawn.

4 In rejecting **claim 23**, the Office asserts that Herbert teaches a computer-  
5 readable medium having computer-executable instructions stored thereon to cause  
6 a server computer to perform a method of entering into a secure connection with a  
7 client computer, obtaining a session key specific to the secure connection,  
8 encrypting data with the session key, and downloading the encrypted data to the  
9 client computer. However, as discussed above with respect to claim 1, Herbert  
10 teaches a secure method of paging within a computer. Herbert does not discuss  
11 downloading data as between a server computer and a client computer. Herbert  
12 discloses a "method and system for maintaining integrity and confidentiality of  
13 pages paged to an external storage unit from a physically secure environment"  
14 (col. 1, lines 58-60). Therefore, among other things, Herbert does not teach a  
15 server computer "entering into a secure connection with a client computer" or  
16 "downloading the encrypted data to the client computer". For at least these  
17 reasons, claim 23 is not anticipated by Herbert, and the §102(b) rejection of claim  
18 23 should be withdrawn.

19 In rejecting **claim 24**, the Office asserts, among other things, that Herbert  
20 teaches computer-executable instructions that cause a client computer to enter into  
21 a secure connection with a server computer. However, as discussed above,  
22 Herbert teaches maintaining the integrity of pages paged to an external storage  
23 unit from a physically secure environment within the context of a virtual memory  
24 system in a single computer. Nowhere does Herbert discuss a client computer  
25 entering into a secure connection with a server computer. Among other things,

1 Applicant's claim 24 recites "computer-executable instructions . . . to cause a  
2 client computer to perform a method comprising: entering into a secure connection  
3 with a server computer". Herbert does not teach the elements of Applicant's claim  
4 24. For at least these reasons, claim 24 is not anticipated by Herbert, and the  
5 §102(b) rejection of claim 24 should be withdrawn.  
6

### 7 **Allowable Subject Matter**

8 Applicant appreciates the allowance of claims 18-22.  
9

### 10 **Claim Objections**

11 Claims 3-4 and 6-12 are objected to as being dependent upon rejected base  
12 claim 1. Claims 15-17 are objected to as being dependent upon rejected base  
13 claim 14. Because base claims 1 and 14 are allowable as discussed herein above,  
14 dependent claims 3-4, 6-12 and 15-17 are also allowable by virtue of their  
15 respective dependencies from base claims 1 and 14.  
16

### 17 **Conclusion**

18 All pending claims are in condition for allowance. Applicant respectfully  
19 requests reconsideration and prompt issuance of the subject application. If any  
20 issues remain that prevent issuance of this application, the Examiner is urged to  
21 contact the undersigned attorney before issuing a subsequent Action.  
22  
23  
24  
25



Respectfully Submitted,

Dated: 3/4/02

By: Nathan R. Rieth  
Nathan R. Rieth  
Reg. No. 44302  
(509) 324-9256

EV052702738



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED  
MAR 14 2002  
2800

Application Serial No. ....  
Filing Date .....  
Inventorship .....  
Applicant ..... Microsoft Corporation  
Group Art Unit ..... 2662  
Examiner ..... Jack, Todd M.  
Attorney's Docket No. .... MS1-282USC3  
Title: Key-Based Secure Storage

22801  
PATENT TRADEMARK OFFICE

Amended Claims With Markings To Show Changes Made

Claims 1, 2, 8, 11, 12 and 18-22 have been changed by the accompanying Response To Office Action relative to their immediate prior versions. A marked up version of claims 1, 2, 8, 11, 12 and 18-22 is therefore submitted below in accordance with 37 C.F.R. §1.121(c).

RECEIVED  
MAR 19 2002  
Technology Center 2100

1. (Amended) A computerized method for key-based secure storage comprising:  
  
    downloading information [content] and an access predicate that specifies requirements for an application to access the information [content];  
  
    obtaining a storage key;  
  
    encrypting the information [content] using the storage key; and  
  
    associating the access predicate with the encrypted information [content].

RECEIVED  
MAR 14 2002  
Technology Center 2600

2. (Amended) The computerized method of claim 1, further comprising:

1           decrypting the information [content] for access by an application  
2 only if the application meets the requirements specified in the access predicate.

3  
4           8.     (Amended) The computerized method of claim 1, wherein the  
5 storage key comprises an application storage key and a user storage key to encrypt  
6 information [content] containing portion specific to an application and a portion  
7 specific to a user, and obtaining the storage key comprises:

8                   generating a seed value for the application;

9                   producing an application hash seed value based on the seed value for  
10 the application using an application-specific one-way hash function;

11                  generating an application storage key from the application hash seed  
12 value;

13                  generating a seed value for the user;

14                  producing a first user hash seed value based on the seed value for the  
15 user using a one-way hash function;

16                  producing a second user hash seed value based on the first user hash  
17 seed value and a user identifier using a keyed hash function; and

18                  generating a user storage key from the second user hash seed value.

19  
20           11.    (Amended) The computerized method of claim 9, further  
21 comprising:

22                  selecting the key vault from a plurality of key vaults provided by a  
23 trusted [digital rights management] operating system.

1 12. (Amended) The computerized method of claim 9, further  
2 comprising:

3 selecting the key vault designated by a provider of the information  
4 [content].

5  
6 18. (Amended) A computer system comprising:  
7 a processing unit;  
8 a system memory coupled to the processing unit through a system  
9 bus;

10 a computer-readable medium coupled to the processing unit through  
11 a system bus; and

12 a trusted [digital rights management] operating system executed  
13 from the computer-readable medium by the processing unit, wherein the trusted  
14 [digital rights management] operating system causes the processing unit to encrypt  
15 downloaded information [content] using a storage key based on a seed value.

16  
17 19. (Amended) The computer system of claim 18, wherein the trusted  
18 [digital rights management] operating system further causes the processing unit to  
19 encrypt an access predicate associated with the downloaded information [content]  
20 using an operating system storage key, to encrypt the seed value for the storage  
21 key using the operating system storage key, and to associate the encrypted access  
22 predicate with the encrypted seed value.

23  
24 20. (Amended) The computer system of claim 19, wherein the trusted  
25 [digital rights management] operating system further causes the processing unit to

1 validate each application requesting access to the downloaded information  
2 [content] using the access predicate, and decrypts the seed value for use by a  
3 validated application.  
4

5 21. (Amended) The computer system of claim 18, wherein the storage  
6 key used to encrypt the downloaded information [content] is specific to an  
7 application.  
8

9 22. (Amended) The computer system of claim 18, wherein the storage  
10 key used to encrypt the downloaded information [content] is specific to a user.  
11  
12  
13  
14

15 Respectfully Submitted,  
16

17 Dated: 3/4/02  
18

19 By: Nathan R Rieth  
20 Nathan R Rieth  
21 Reg. No. 44302  
22 (509) 324-9256; X233  
23  
24  
25